

Отчёт по лабораторной работе 5

Расширенная настройка HTTP-сервера Apache

Авдадаев Джамал Геланиевич

Содержание

1 Введение	5
1.1 Цель работы	5
2 Процесс работы	6
2.1 Конфигурирование HTTP-сервера для работы через протокол HTTPS	6
2.1.1 Построчное пояснение конфигурации	7
2.2 Конфигурирование HTTP-сервера для работы с PHP	9
2.3 Внесение изменений во внутреннее окружение виртуальной машины	11
3 Итоги	13
3.1 Вывод	13
3.2 Контрольные вопросы	13

Список иллюстраций

2.1 Генерация ключа и сертификата	6
2.2 Конфигурация Apache	7
2.3 Работа сайта по HTTPS	9
2.4 Просмотр сертификата	9
2.5 Файл index.php	10
2.6 Отображение phpinfo	10
2.7 Копирование конфигурационных файлов	11
2.8 Изменения в скрипте http.sh	12

Список таблиц

1 Введение

1.1 Цель работы

Целью данной работы является приобретение практических навыков установки Rocky Linux на виртуальную машину с помощью инструмента Vagrant.

2 Процесс работы

2.1 Конфигурирование HTTP-сервера для работы через протокол HTTPS

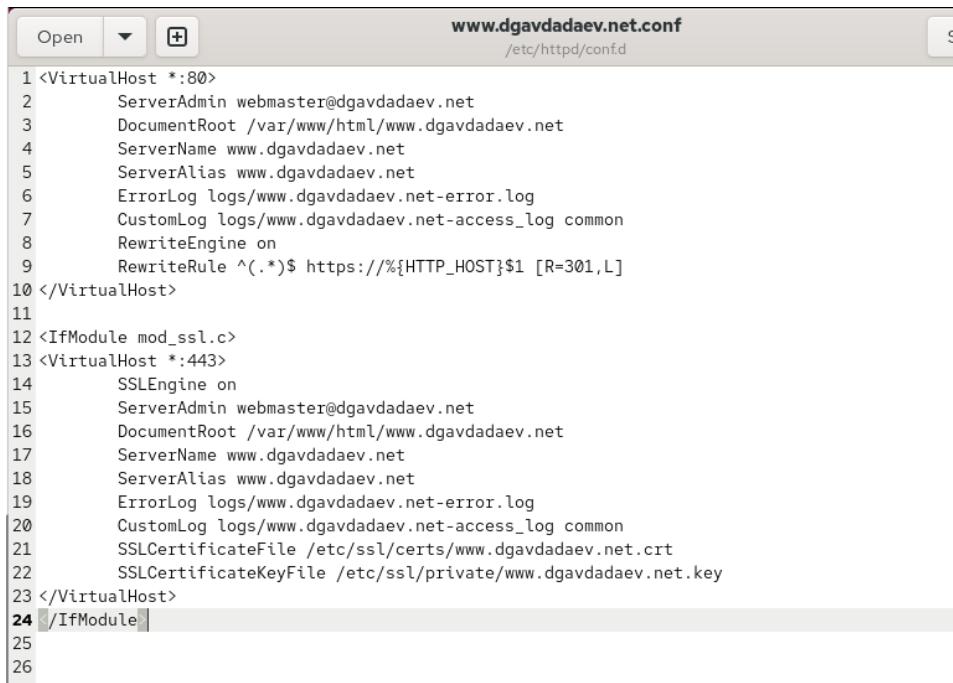
В каталоге `/etc/pki/tls/private` был создан приватный ключ и самоподписанный сертификат для домена **www.dgavdadaev.net**. Использовалась команда генерации сертификата, после чего были введены параметры: RU, Russia, Moscow, dgavdadaev, dgavdadaev, dgavdadaev.net, dgavdadaev@dgavdadaev.net.

```
[root@server.dgavdadaev.net private]# openssl req -x509 -nodes -newkey rsa:2048 -keyout www.dgavdadaev.key -out www.dgavdadaev.crt
-----+
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [XX]:RU
State or Province Name (full name) []:Russia
Locality Name (eg, city) [Default City]:Moscow
Organization Name (eg, company) [Default Company Ltd]:dgavdadaev
Organizational Unit Name (eg, section) []:dgavdadaev
Common Name (eg, your name or your server's hostname) []:dgavdadaev.net
Email Address []:dgavdadaev@dgavdadaev.net
[root@server.dgavdadaev.net private]# ls
localhost.key www.dgavdadaev.crt www.dgavdadaev.key
[root@server.dgavdadaev.net private]#
[root@server.dgavdadaev.net private]# mv www.dgavdadaev.crt www.dgavdadaev.net.crt
[root@server.dgavdadaev.net private]# mv www.dgavdadaev.key www.dgavdadaev.net.key
[root@server.dgavdadaev.net private]# cp www.dgavdadaev.net.crt /etc/ssl/certs/
[root@server.dgavdadaev.net private]#
```

Рис. 2.1: Генерация ключа и сертификата

Сертификат и ключ были переименованы и размещены в соответствующих каталогах. Далее сертификат был скопирован в /etc/ssl/certs/.

Был отредактирован файл `/etc/httpd/conf.d/www.dgavdadaev.net.conf`, после чего он получил следующий вид:



```
www.dgavdadaev.net.conf
/etc/httpd/conf.d

1 <VirtualHost *:80>
2     ServerAdmin webmaster@dgavdadaev.net
3     DocumentRoot /var/www/html/www.dgavdadaev.net
4     ServerName www.dgavdadaev.net
5     ServerAlias www.dgavdadaev.net
6     ErrorLog logs/www.dgavdadaev.net-error.log
7     CustomLog logs/www.dgavdadaev.net-access_log common
8     RewriteEngine on
9     RewriteRule ^(.*)$ https:// %{HTTP_HOST}$1 [R=301,L]
10 </VirtualHost>
11
12 <IfModule mod_ssl.c>
13 <VirtualHost *:443>
14     SSLEngine on
15     ServerAdmin webmaster@dgavdadaev.net
16     DocumentRoot /var/www/html/www.dgavdadaev.net
17     ServerName www.dgavdadaev.net
18     ServerAlias www.dgavdadaev.net
19     ErrorLog logs/www.dgavdadaev.net-error.log
20     CustomLog logs/www.dgavdadaev.net-access_log common
21     SSLCertificateFile /etc/ssl/certs/www.dgavdadaev.net.crt
22     SSLCertificateKeyFile /etc/ssl/private/www.dgavdadaev.net.key
23 </VirtualHost>
24 </IfModule>
25
26
```

Рис. 2.2: Конфигурация Apache

2.1.1 Построчное пояснение конфигурации

- `<VirtualHost *:80>` — начало конфигурации виртуального хоста для HTTP.
- `ServerAdmin webmaster@dgavdadaev.net` — адрес администратора.
- `DocumentRoot /var/www/html/www.dgavdadaev.net` — корневая директория сайта.
- `ServerName` и `ServerAlias` — доменное имя сайта.

- `ErrorLog` и `CustomLog` – файлы логирования ошибок и обращений.
- `RewriteEngine on` – включение механизма переписывания ссылок.
- `RewriteRule ^(.*)$ https:// %{HTTP_HOST}$1 [R=301,L]` – принудительное перенаправление всех запросов на HTTPS.
- `</VirtualHost>` – завершение блока HTTP.
- `<IfModule mod_ssl.c>` – проверка наличия модуля SSL.
- `<VirtualHost *:443>` – начало конфигурации HTTPS.
- `SSLEngine on` – включение SSL.
- Повторяются параметры администратора, домена, корневого каталога и логов.
- `SSLCertificateFile` – путь к сертификату.
- `SSLCertificateKeyFile` – путь к приватному ключу.
- `</VirtualHost>` – конец конфигурации HTTPS.
- `</IfModule>` – завершение условного блока.

После перезапуска веб-сервера сайт стал доступен по защищённому протоколу HTTPS.

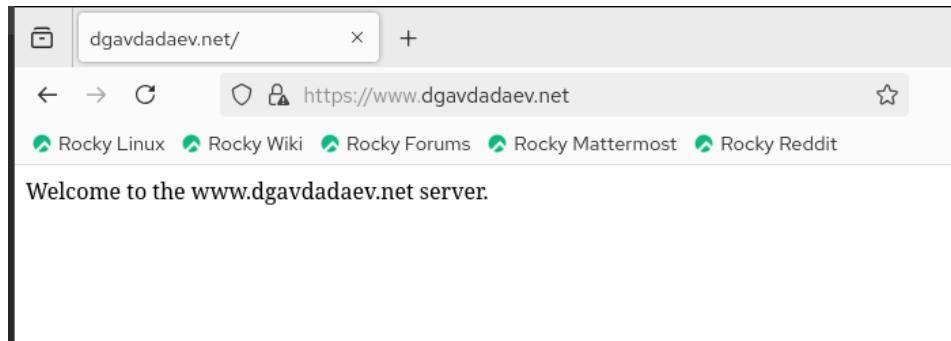


Рис. 2.3: Работа сайта по HTTPS

Просмотр сведений о сертификате показал корректность введённых параметров.

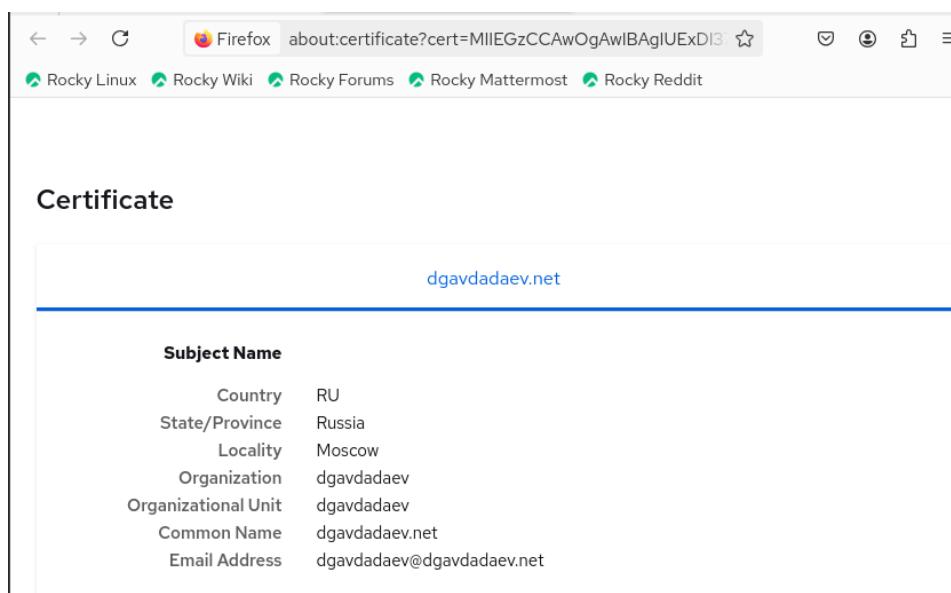
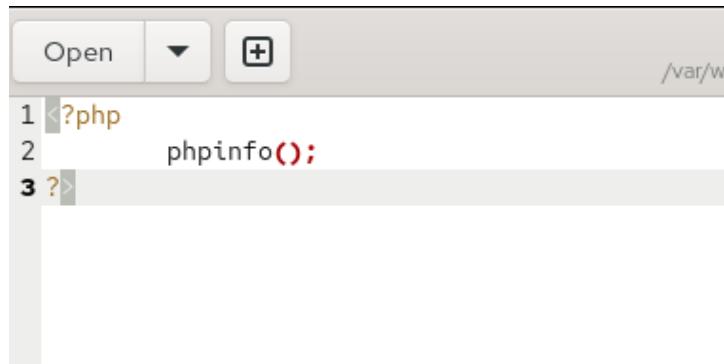


Рис. 2.4: Просмотр сертификата

2.2 Конфигурирование HTTP-сервера для работы с PHP

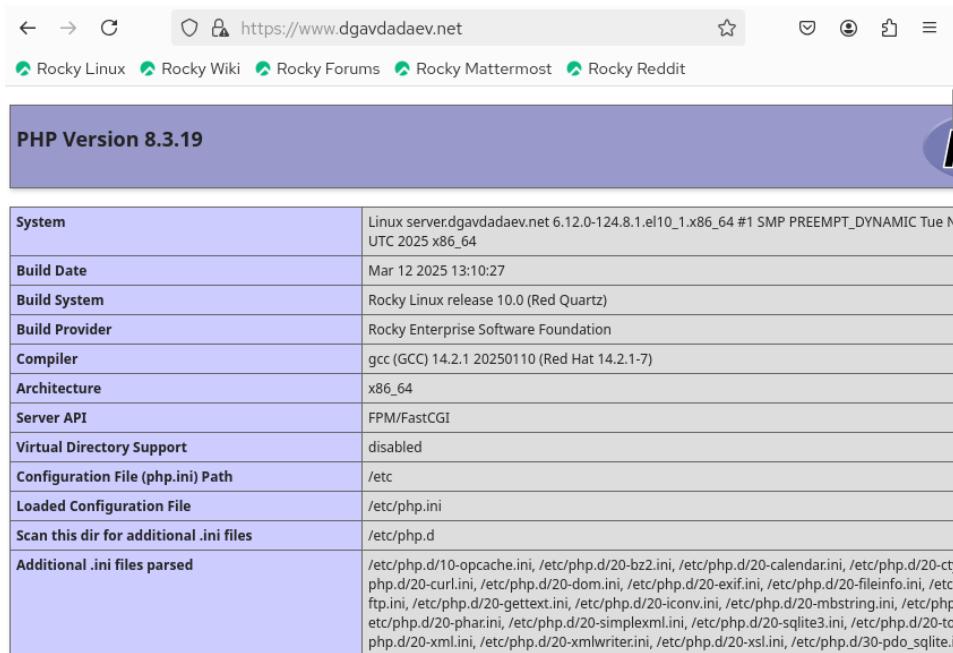
В каталоге сайта был создан файл `index.php` с функцией `phpinfo()`.



```
1 <?php
2      phpinfo();
```

Рис. 2.5: Файл index.php

После выполнения всех настроек веб-сервер корректно обработал PHP-страницу.



PHP Version 8.3.19

System	Linux server.dgavdadaev.net 6.12.0-124.8.1.el10_1.x86_64 #1 SMP PREEMPT_DYNAMIC Tue Nov 14 14:20:00 UTC 2025 x86_64
Build Date	Mar 12 2025 13:10:27
Build System	Rocky Linux release 10.0 (Red Quartz)
Build Provider	Rocky Enterprise Software Foundation
Compiler	gcc (GCC) 14.2.1 20250110 (Red Hat 14.2.1-7)
Architecture	x86_64
Server API	FPM/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc
Loaded Configuration File	/etc/php.ini
Scan this dir for additional .ini files	/etc/php.d
Additional .ini files parsed	/etc/php.d/10-opcache.ini, /etc/php.d/20-bz2.ini, /etc/php.d/20-calendar.ini, /etc/php.d/20-ctype.ini, /etc/php.d/20-curl.ini, /etc/php.d/20-dom.ini, /etc/php.d/20-exif.ini, /etc/php.d/20-fileinfo.ini, /etc/php.d/20-ftp.ini, /etc/php.d/20-gettext.ini, /etc/php.d/20-iconv.ini, /etc/php.d/20-mbstring.ini, /etc/php.d/20-phar.ini, /etc/php.d/20-simplexml.ini, /etc/php.d/20-sqlite3.ini, /etc/php.d/20-xml.ini, /etc/php.d/20-xmlwriter.ini, /etc/php.d/20-xsl.ini, /etc/php.d/30-pdo_sqlite.ini

Рис. 2.6: Отображение phpinfo

2.3 Внесение изменений во внутреннее окружение виртуальной машины

В каталоге `/vagrant/provision/server/http` были размещены актуальные конфигурации веб-сервера. Для этого скопированы файлы Apache, веб-контента и SSL-материалов:

- конфигурации `/etc/httpd/conf.d/*` перенесены в `.../etc/httpd/conf.d/`;
- содержимое веб-каталога `/var/www/html/*` – в `.../var/www/html/`;
- созданы каталоги для ключей и сертификатов `etc/pki/tls/private` и `etc/pki/tls/certs`;
- файл приватного ключа и файл сертификата перенесены в соответствующие пути внутри `provision`.

```
[root@server.dgavdadaev.net www.dgavdadaev.net]# cp -R /etc/httpd/conf.d/* /vagrant/provision/server/http/etc/httpd/conf.d/
cp: overwrite '/vagrant/provision/server/http/etc/httpd/conf.d/autoindex.conf'? y
cp: overwrite '/vagrant/provision/server/http/etc/httpd/conf.d/fcgid.conf'? y
cp: overwrite '/vagrant/provision/server/http/etc/httpd/conf.d/manual.conf'? y
cp: overwrite '/vagrant/provision/server/http/etc/httpd/conf.d/README'? y
cp: overwrite '/vagrant/provision/server/http/etc/httpd/conf.d/server.dgavdadaev.net.conf'? y
cp: overwrite '/vagrant/provision/server/http/etc/httpd/conf.d/ssl.conf'? y
cp: overwrite '/vagrant/provision/server/http/etc/httpd/conf.d/userdir.conf'? y
cp: overwrite '/vagrant/provision/server/http/etc/httpd/conf.d/welcome.conf'? y
cp: overwrite '/vagrant/provision/server/http/etc/httpd/conf.d/www.dgavdadaev.net.conf'? y
[vroot@server.dgavdadaev.net www.dgavdadaev.net]# cp -R /var/www/html/* /vagrant/provision/server/http/var/www/html/
cp: overwrite '/vagrant/provision/server/http/var/www/html/server.dgavdadaev.net/index.html'? y
[root@server.dgavdadaev.net www.dgavdadaev.net]#
[root@server.dgavdadaev.net www.dgavdadaev.net]# mkdir -p /vagrant/provision/server/http/etc/pki/tls/private
[root@server.dgavdadaev.net www.dgavdadaev.net]# cp -R /etc/pki/tls/private/www.dgavdadaev.net.key /vagrant/provision/server/http/etc/pki/tls/private
[root@server.dgavdadaev.net www.dgavdadaev.net]# mkdir -p /vagrant/provision/server/http/etc/pki/tls/certs
[root@server.dgavdadaev.net www.dgavdadaev.net]# cp -R /etc/pki/tls/private/www.dgavdadaev.net.crt /vagrant/provision/server/http/etc/pki/tls/certs
[root@server.dgavdadaev.net www.dgavdadaev.net]#
```

Рис. 2.7: Копирование конфигурационных файлов

В скрипт `/vagrant/provision/server/http.sh` добавлены команды для установки PHP и правил межсетевого экрана, позволяющих работать через HTTPS. Это обеспечивает автоматическую подготовку окружения при развёртывании.

```
1  #!/bin/bash
2  echo "Provisioning script $0"
3  echo "Install needed packages"
4  dnf -y groupinstall "Basic Web Server"
5  dnf -y install php
6
7  echo "Copy configuration files"
8  cp -R /vagrant/provision/server/http/etc/httpd/* /etc/httpd
9  cp -R /vagrant/provision/server/http/var/www/* /var/www
10 chown -R apache:apache /var/www
11 restorecon -vR /etc
12 restorecon -vR /var/www
13 echo "Configure firewall"
14 firewall-cmd --add-service=http
15 firewall-cmd --add-service=http --permanent
16 firewall-cmd --add-service=https
17 firewall-cmd --add-service=https --permanent
18 echo "Start http service"
19 systemctl enable httpd
20 systemctl start httpd
21
```

Рис. 2.8: Изменения в скрипте http.sh

3 ИТОГИ

3.1 Вывод

В процессе работы был настроен веб-сервер для функционирования через HTTPS, создан самоподписанный сертификат, выполнено перенаправление с HTTP на HTTPS и добавлена поддержка PHP. Конфигурации и SSL-материалы перенесены во внутреннее окружение виртуальной машины для автоматического развертывания. Проверена работа сертификата и корректное выполнение PHP-скриптов.

3.2 Контрольные вопросы

1. В чём отличие HTTP от HTTPS?

HTTP передаёт данные в открытом виде, тогда как HTTPS использует шифрование (TLS/SSL), обеспечивая защищённый канал между сервером и клиентом.

2. Каким образом обеспечивается безопасность контента веб-сервера при работе через HTTPS?

Безопасность достигается за счёт шифрования трафика, проверки подлинности сервера с помощью сертификата и защиты данных от перехвата и изменения.

3. Что такое сертификационный центр? Приведите пример.

Сертификационный центр (CA) – организация, выпускающая и подписывающая цифровые сертификаты, подтверждая подлинность владельца.

Примеры: LetsEncrypt, DigiCert, GlobalSign.